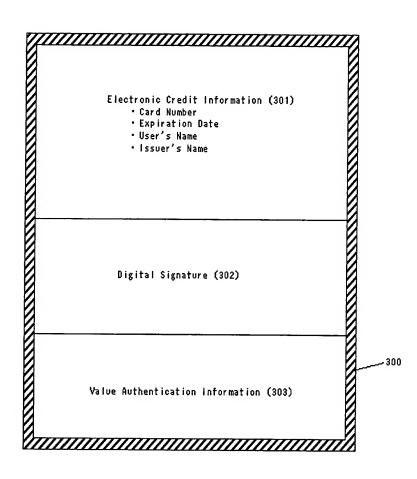
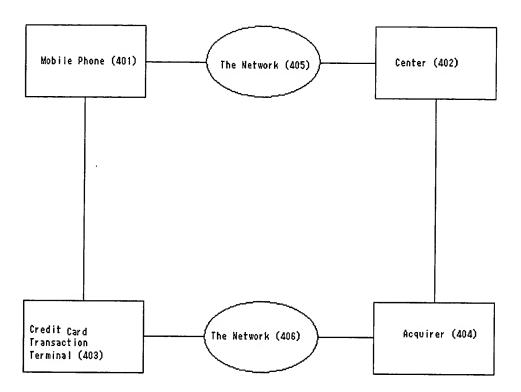
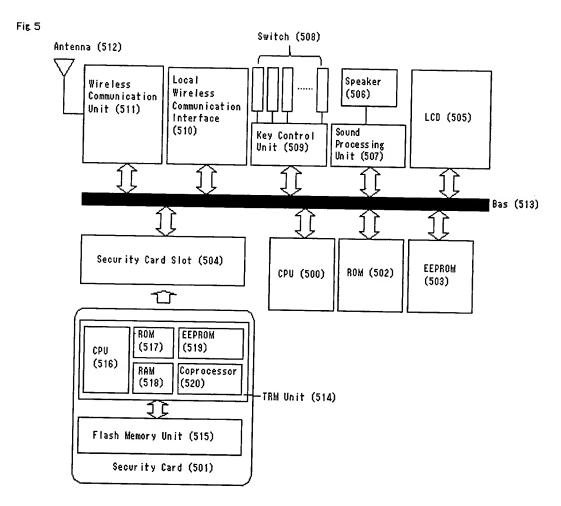


Fig. 3







..

Fig. 6

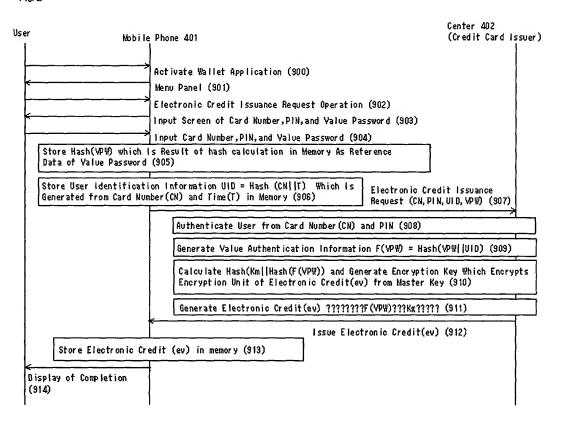
			Electi	onic Credit Inform	nation List (601)
Card Type #	Master Key #4	Certificate of Credit Card Issuer #4	Negative List #4	Acquirer Information #4	Risk Management Information #4
Card Type	#3 Master Key #3	Certificate of Credit Card Issuer #3	Negative List #3	Acquirer Information #3	Risk Management Information #3
Card Type	#2 Master Key #2	Certificate of Credit Card Issuer #2	Negative List #2	Acquirer Information #2	Risk Management Information #2
Card Type	#1 Master Key #1	Certificate of Credit Card Issuer #1	Negative List #1	Acquirer Information #1	Risk Management Information #1

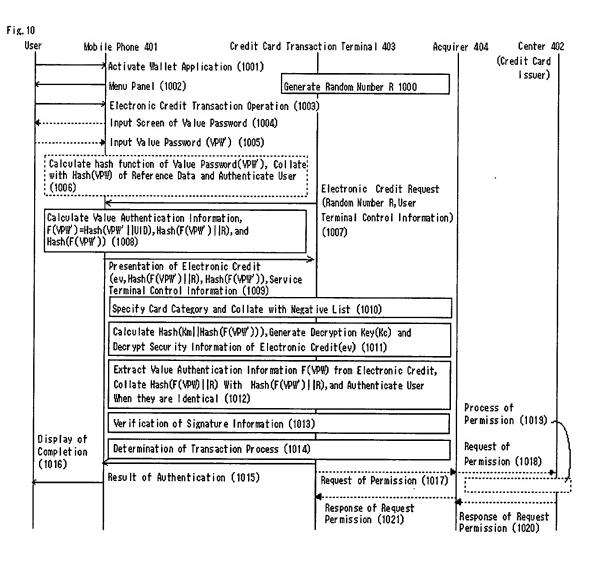
Flash Memory Unit (515)

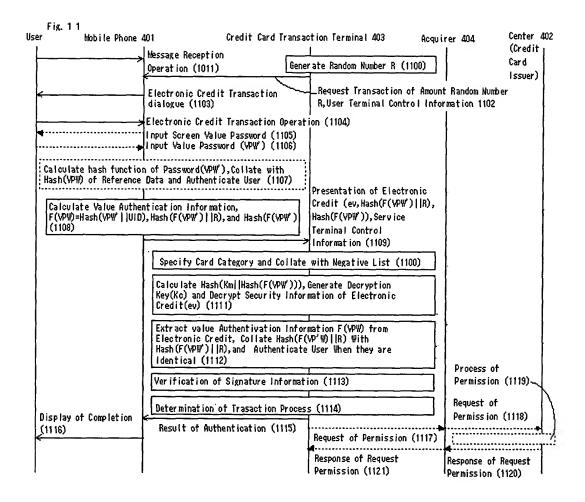
Fig. 7

Wallet Display Information (701)	Wallet Sound Information (702)
L	

Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Credit #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Credit #3	Property #3







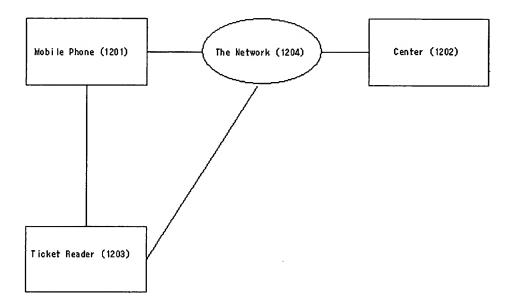


Fig. 13

•

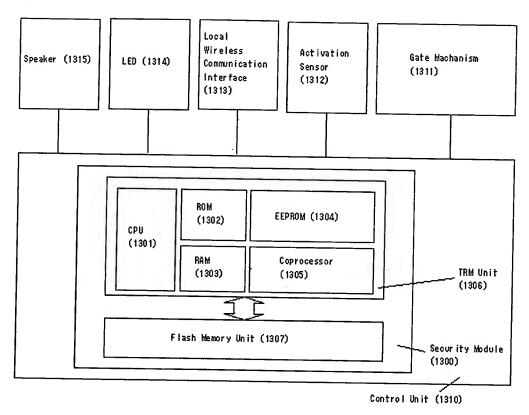


Fig. 14

Ticket Type #1	Master Key #1	Certificate of Ticket Issuer #1	Negative List #1
Ticket Type #2	Master Key #2	Certificate of Ticket Issuer #2	Negative List #2
Ticket Type #3	Master Key #3	Certificate of Ticket Issuer #3	Negative List #3
Ticket Type #4	Master Key #4	Certificate of Ticket Issuer #4	Negative List #4
	Ticket Reading H	Electronic Ticket Informat	ion List (1401)

∖Flash Memory Unit (1407)

Fig. 15

Wallet Display Information (150	1) Wallet Sound Information (1502)

Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
	User Identification Information #2	Electronic Credit #2	Property #2

Reference Data #1	User Identification Information #1	Electronic Ticket #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Ticket #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Ticket #3	Property #3

Electronic Ticket Public Information
(1601)

• Ticket Attribute Information
• Expiration Date
• Issuer's Name

Electronic Ticket Secret Information (1602)

Value Authentication Information (1603)

Security Information (1600)

Display Information (1605)



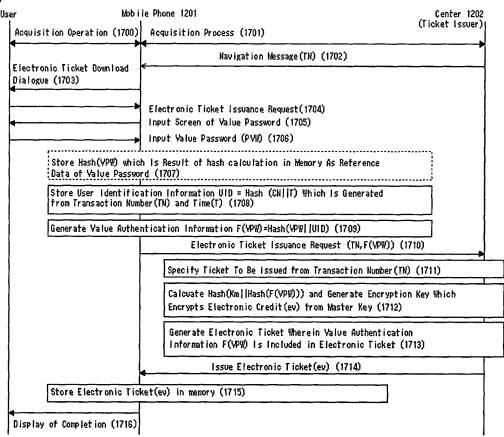


Fig. 18 User Ticket Reader 1203 Mobile Phone 1201 🖊 Activate Wallet Application (1801) Menu Panel (1802) Generate Random Number R1 (1800) Electronic Ticket Usage Operation (1803) input Screen of Value Password (1804) Input Value Password(VPW') (1805) Calculate hash function of Value Password(VPW'), Collate with Hash(VPW) of Reference Data and Authenticate User (1806) Electronic Credit Presentation Request Generate Random Number R2 (1808) (Random Number R1, User Terminal Control Information) (1807) Calculate Value Authentication Information F(VPW')=Hash(VPW'||UID),Hash(F(VPW'||R),and Hash(F(VPW')) (1809) Presentation of Electronic Specify Ticket Category and Collate with Negative List (1811) Credit (ev, Hash(F(VPW')||R1), Hash(F(VPW')), R2, Service Calculate Hash(Km||Hash(F(YPW'))), Generate Decryption Key(Kt) and Terminal Control Decrypt Security Information of Electronic Ticket(ev) (1812) Information) (1810) Extract Value Authentication Information F(VPW) from Electronic Credit, Collate Hash(F(VPW)||R1) With Hash(F(VPW')||R1), and Authenticate User When They Are Identical (1813) Verification of Signature Information (1814) Change Electronic Ticket Disclosure Information and Electronic Ticket Secret Information to The State After Ticket Examination and Generate Electronic Ticket(ev') Which Is Operated Examination Process (1815) Electronic Ticket Updating Request(ev'), Calculate Hash(F(VPW)||R1||R2) (1816) Hash(F(VPW)||R1||R2) (1817) Collate Hash(F(VPW')||R1||R2) with Hash(F(VPW)||R1||R2) and Authenticate Ticket Examiner When They Are Identical (1818). Update Electronic Ticket to Received and Examined Electronic Ticket(ev') (1919) Update Notification 1820 Display of Completion (1822) Ticket Reading Termination Operation (1821)

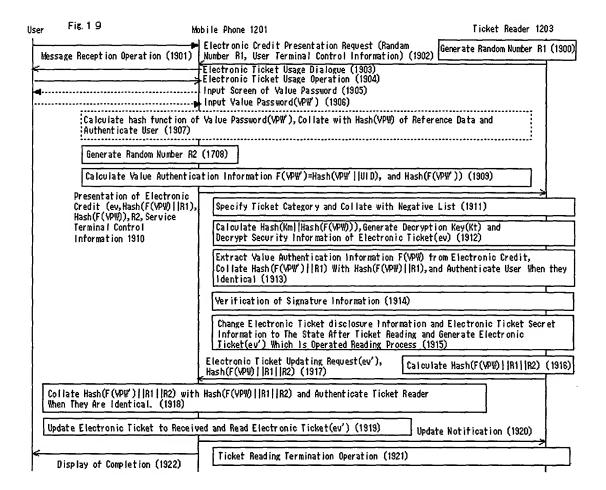


Fig. 20

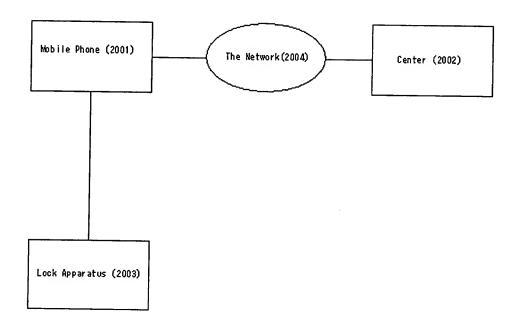
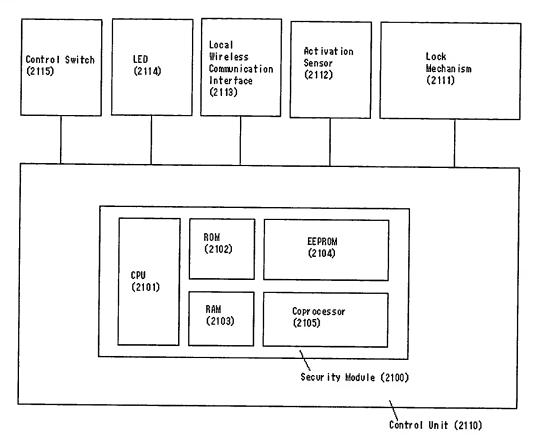


Fig. 21



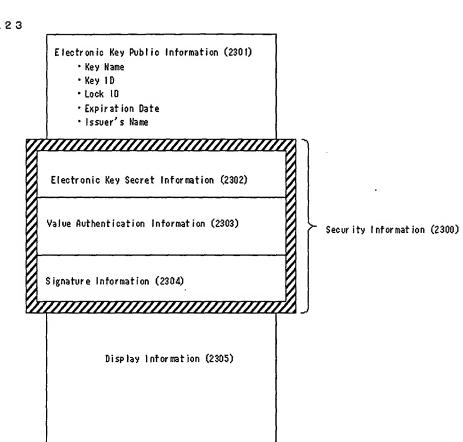
Wallet Display Information (2201)	Wallet Sound Information (2202)

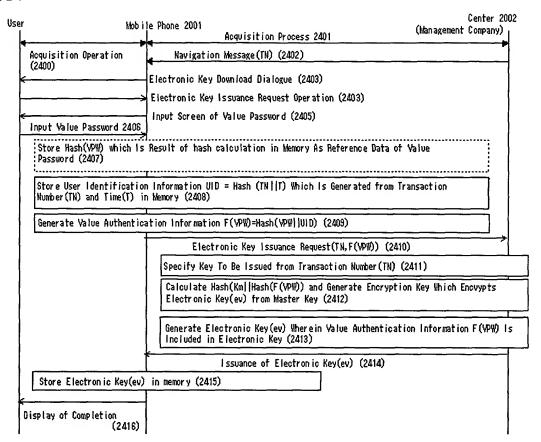
lectronic Credit Li	st (2203)		
Reference Data #1	User Identification Information #1	Electronic Credit #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Credit #2	Property #2

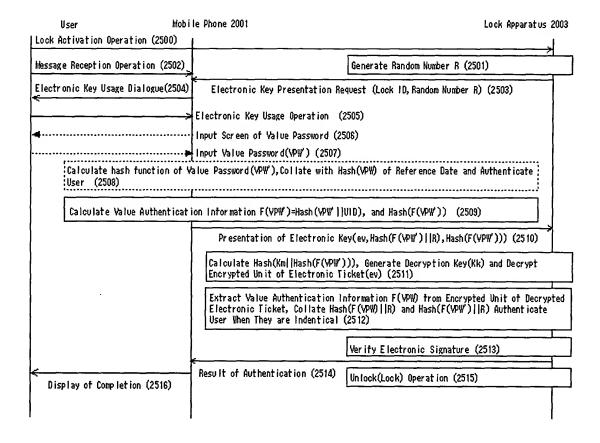
Reference Data #1	User Identification Information #1	Electronic Ticket #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Ticket #2	Property #2

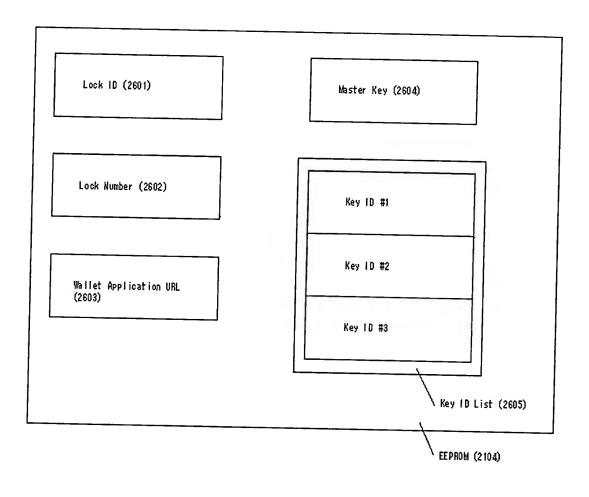
Reference Data #1	User Identification Information #1	Electronic Key #1	Property #1
Reference Data #2	User Identification Information #2	Electronic Key #2	Property #2
Reference Data #3	User Identification Information #3	Electronic Key #3	Property #3

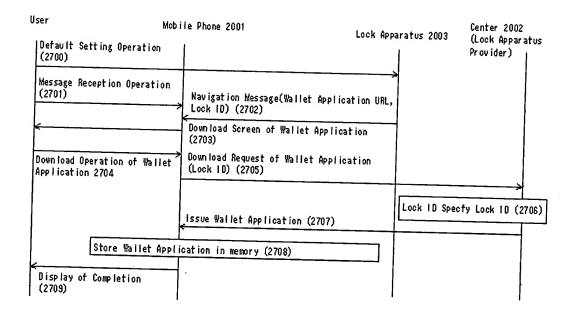


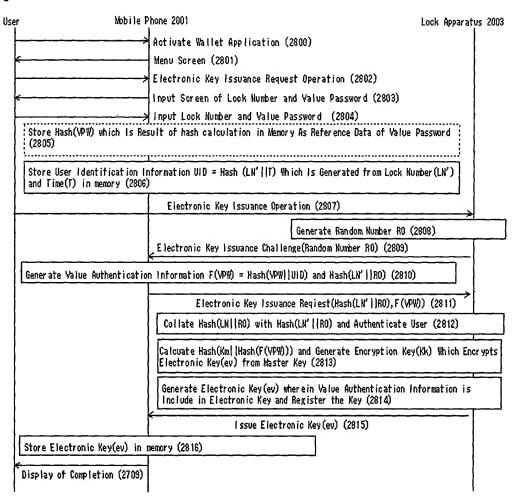


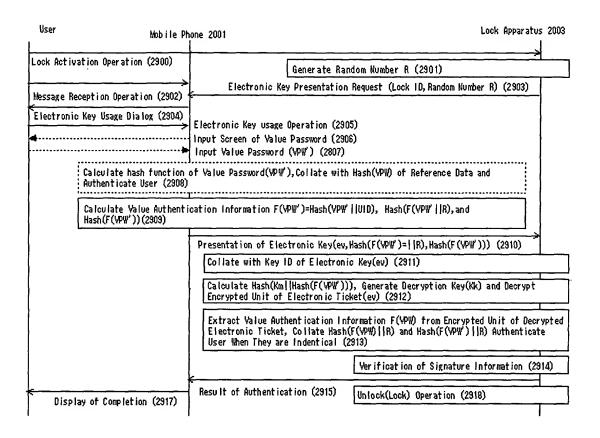












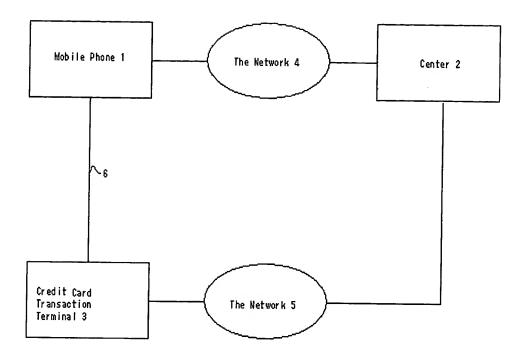


Fig. 3 1

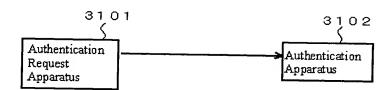
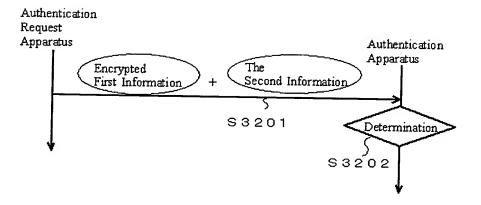


Fig 3 2



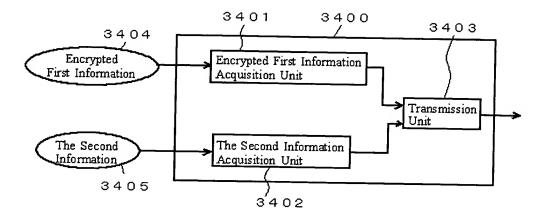
(A)

Encrypted First Informaiton	Encrypt (Password)
The Second Information	Password
Condition of Determination	Decrypt (Encrypted First Information) = The Second Information?

(B)

Encrypted First Information	Encrypt (Password)
The Second Information	F (Password)
Condition of Determination	F (Decrypt (Encrypted First Information)) = The Second Information?

Fig 3 4

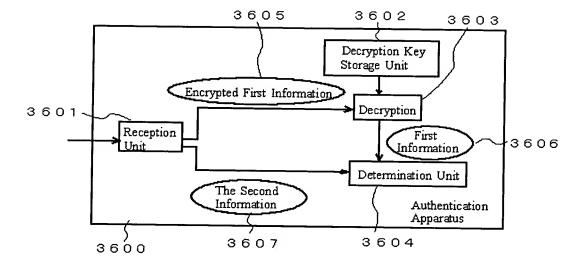


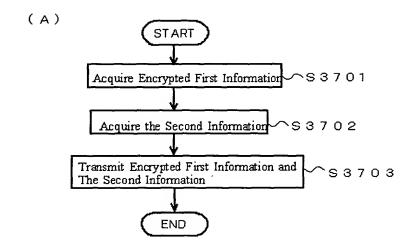
(A)

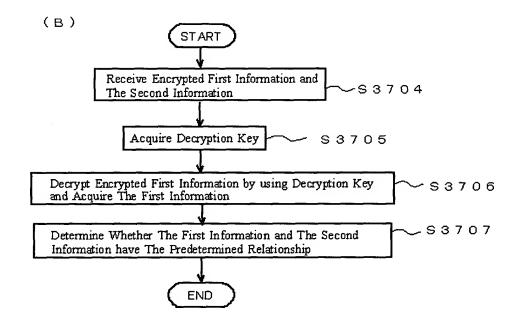
The First Information
Encryption

The First Information + Additional Information

Encryption







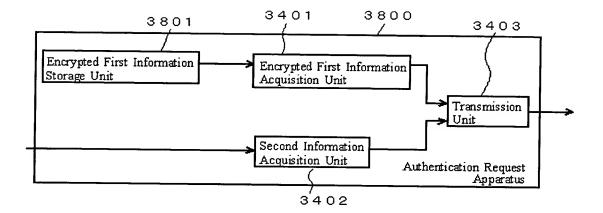
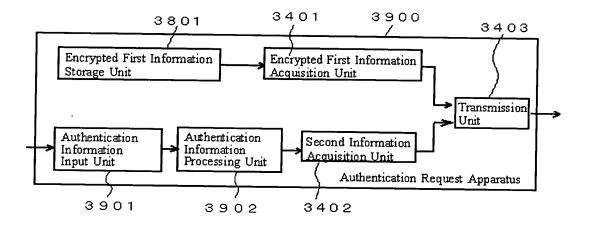
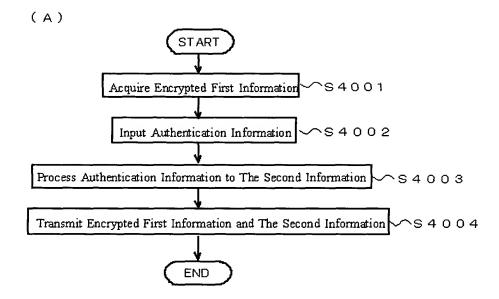
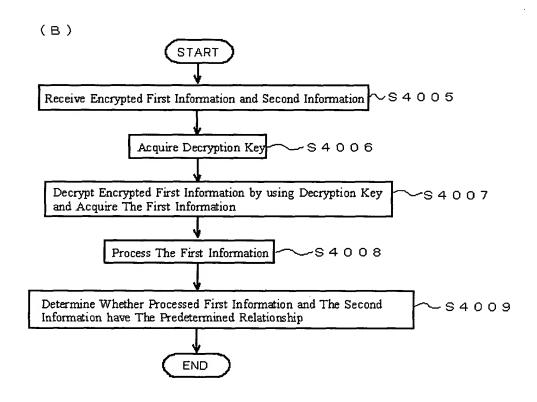


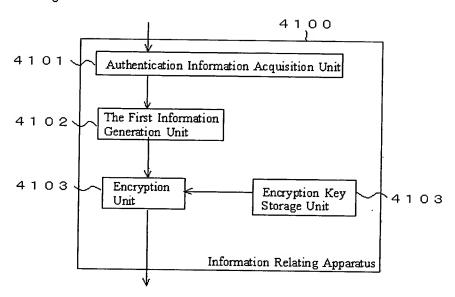
Fig. 3 9

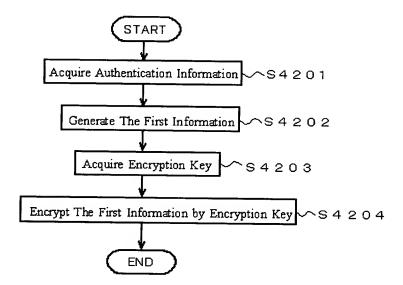


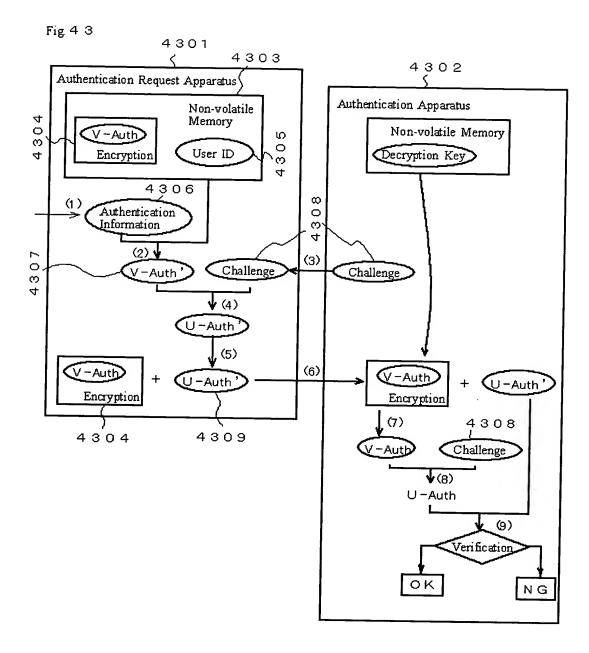












- (1) V-Auth=Hash1 (Password || User ID)
- (2) V-Auth'=Hash1 (Authentication Information | User ID)
- (3) U-Auth'≡Hash₂(V-Auth'∥ Challenge)
- (4) U-Auth = Hash2 (V-Auth || Challenge)